

$\mathbb{Z}_p\mathbb{Z}_p[u]$ -additive codes*

Zhenliang Lu, Shixin Zhu

Department of Mathematics, Hefei University of Technology, Hefei 230009, Anhui, P.R.China

Abstract: In this paper, we study $\mathbb{Z}_p\mathbb{Z}_p[u]$ -additive codes, where p is prime and $u^2 = 0$. In particular, we determine a Gray map from $\mathbb{Z}_p\mathbb{Z}_p[u]$ to $\mathbb{Z}_p^{\alpha+2\beta}$ and study generator and parity check matrices for these codes. We prove that a Gray map Φ is a distance preserving map from $(\mathbb{Z}_p\mathbb{Z}_p[u], \text{Gray distance})$ to $(\mathbb{Z}_p^{\alpha+2\beta}, \text{Hamming distance})$, it is a weight preserving map as well. Furthermore we study the structure of $\mathbb{Z}_p\mathbb{Z}_p[u]$ -additive cyclic codes.

Keywords: additive codes; $\mathbb{Z}_p\mathbb{Z}_p[u]$ -additive codes; $\mathbb{Z}_p\mathbb{Z}_p[u]$ -additive cyclic codes; Gray map.

1 Introduction

Additive codes with the remarkable paper by Delsarte in 1973[1], he defines additive codes as subgroups of the underlying abelian group in a translation association scheme. In 2006, Borges J. et al. define an extension of the usual Gray map, the new Gray map is an isometry which transforms Lee distance in $Z_2^\alpha \times Z_4^\beta$ to Hamming distance in $Z_2^{\alpha+2\beta}$ [6]. Then, many properties of additive codes are studied. Two kinds of maximum distance separable codes over Z_2Z_4 are studied[7], all MDS Z_2Z_4 -additive codes are zero or one error-correcting codes with the exception of the trivial repetition codes containing two codewords. Cyclic additive codes are also studied[8][15]. Recently, Z_2Z_4 -additive codes were generalized to $Z_2Z_{2^s}$ -additive codes by Aydogdu and Siap[9]. And next $Z_{p^r}Z_{p^s}$ -additive codes are studied by Aydogdu and Siap[4]. In [4], the paper given the standard generator matrices and dual matrices of the form over $Z_{p^r}Z_{p^s}$ -additive codes.

Later, in [3], a generalization towards another direction that have a good algebraic structure and provide good binary codes is presented, a new class of additive codes which is referred to as $Z_2Z_2[u]$ -additive codes is introduced. About the application of additive codes to steganography is proposed[10] and It's also helped to study quantum code. Now, quantum additive code is a new research direction. Many articles and research has been done on quantum additive codes. In this paper, we extend the $Z_2Z_2[u]$ -additive codes to codes over $\mathbb{Z}_p\mathbb{Z}_p[u]$, where p is prime and $u^2 = 0$. Corresponding, we given a more simplify standard generator matrices and dual matrices of the form. At the same time, we define a Gray map Φ . We prove that a Gray map Φ is a distance preserving map from $(\mathbb{Z}_p\mathbb{Z}_p[u], \text{Gray distance})$ to $(\mathbb{Z}_p^{\alpha+2\beta}, \text{Hamming distance})$, it is a weight preserving map as well. At the end of the paper, we study the structure of $\mathbb{Z}_p\mathbb{Z}_p[u]$ -additive cyclic codes.

2 Preliminaries

Let \mathbb{Z}_p be a finite field with p elements, where p is an odd prime. Let R be the commutative ring $\mathbb{Z}_p + u\mathbb{Z}_p = \{a + ub \mid a, b \in \mathbb{Z}_p\}$ where $u^2 = 0$. A linear code C over R containing some

* E-mail addresses: luzhenliang1992@sina.cn(Z.lu), zhushixin@hfut.edu.cn(S.Zhu).

This research is supported by the National Natural Science Foundation of China (No.61370089) and the Anhui Provincial Natural Science Foundation under Grant JZ2015AKZR0229.

nonzero codewords is permutation equivalent to a code with a generator matrix of the form

$$G = \begin{pmatrix} I_{k_0} & A & B \\ 0 & uI_{k_1} & uD \end{pmatrix},$$

where A, D are p -ary matrices, B is $\mathbb{Z}_p + u\mathbb{Z}_p$ -matrices, I_{k_0} and I_{k_1} denote the $k_0 \times k_0$ and $k_1 \times k_1$ identity matrices, and C contains $p^{2k_0+k_1}$ codewords[2].

We define a Gray map ψ from R to \mathbb{Z}_p^2 in the following way.

$$\begin{aligned} \psi : R &\rightarrow \mathbb{Z}_p^2 \\ (a + ub) &\rightarrow (b, a + b). \end{aligned}$$

The set $\mathbb{Z}_p\mathbb{Z}_p[u]$ is defined by

$$\mathbb{Z}_p\mathbb{Z}_p[u] = \{(a, b) | a \in \mathbb{Z}_p \text{ and } b \in R\}$$

The set not well defined with respect to the usual multiplication, therefore, to make it well defined and get some good results, we introduce a new scalar multiplication in the following way:

$$(1) \forall c_1 = (a_0, a_1, \dots, a_{\alpha-1}, b_0, b_1, \dots, b_{\beta-1}), c_2 = (a'_0, a'_1, \dots, a'_{\alpha-1}, b'_0, b'_1, \dots, b'_{\beta-1}) \in \mathbb{Z}_p\mathbb{Z}_p[u]$$

$$c_1 c_2 = (a_0 a'_0, a_1 a'_1, \dots, a_{\alpha-1} a'_{\alpha-1}, b_0 b'_0, b_1 b'_1, \dots, b_{\beta-1} b'_{\beta-1})$$

$$(2) \forall c_1 = (a_0, a_1, \dots, a_{\alpha-1}, b_0, b_1, \dots, b_{\beta-1}) \in \mathbb{Z}_p\mathbb{Z}_p[u], c = r + qu \in R.$$

$$cc_1 = (ra_0, ra_1, \dots, ra_{\alpha-1}, cb_0, cb_1, \dots, cb_{\beta-1})$$

$$(3) \forall c_1 = (a_0, a_1, \dots, a_{\alpha-1}, b_0, b_1, \dots, b_{\beta-1}) \in \mathbb{Z}_p\mathbb{Z}_p[u], c \in \mathbb{Z}_p.$$

$$cc_1 = (ca_0, ca_1, \dots, ca_{\alpha-1}, cb_0, cb_1, \dots, cb_{\beta-1})$$

3 $\mathbb{Z}_p\mathbb{Z}_p[u]$ -additive codes

In this section, we introduced the definition of the additive codes and the additive dual codes, determine the structure of the generator matrix and dual generator matrix in the standard form of the code.

Definition 3.1. A linear code C is called a $\mathbb{Z}_p\mathbb{Z}_p[u]$ additive code if it is a $\mathbb{Z}_p + \mathbb{Z}_p[u]$ submodule of $\mathbb{Z}_p^\alpha \times \mathbb{Z}_p[u]^\beta$ with respect to the scalar multiplication defined in (1),(2),(3). Then the p -ary image $\Phi(C) = \mathbf{C}$ is called $\mathbb{Z}_p\mathbb{Z}_p[u]$ linear code of length $n = \alpha + 2\beta$ where Φ is a map from $\mathbb{Z}_p^\alpha \times \mathbb{Z}_p[u]^\beta$ to \mathbb{Z}_p^n defined as

$$\Phi(a, b) = (a_0, a_1, \dots, a_{\alpha-1}, \psi(b_0), \psi(b_1), \dots, \psi(b_{\beta-1}))$$

for all $a = (a_0, a_1, \dots, a_{\alpha-1}) \in \mathbb{Z}_p^\alpha$, $b = (b_0, b_1, \dots, b_{\beta-1}) \in \mathbb{Z}_p[u]^\beta$.

Theorem 3.2. Let C be a $\mathbb{Z}_p\mathbb{Z}_p[u]$ -additive code of type $(p; \alpha, \beta; k_0, k_1)$. Then C is permutation equivalent to a $\mathbb{Z}_p\mathbb{Z}_p[u]$ additive code with the standard form matrix

$$G = \begin{pmatrix} I_{k_0} & A & B \\ 0 & uI_{k_1} & uD \end{pmatrix}, \quad (1)$$

where A, B, D are R -matrices, I_{k_0} and I_{k_1} denote the $k_0 \times k_0$ and $k_1 \times k_1$ identity matrices.

Proof Since the $\mathbb{Z}_p\mathbb{Z}_p[u]$ additive codes front part is \mathbb{Z}_p^α , so the $\mathbb{Z}_p\mathbb{Z}_p[u]$ additive codes can be generated by a matrix as follow:

$$\begin{pmatrix} I_{k_0} & S_1 \end{pmatrix},$$

where S are Z_P -matrix.

Likewise, the $\mathbb{Z}_p\mathbb{Z}_p[u]$ additive codes after part is $\mathbb{Z}_p + u\mathbb{Z}_p$, so the $\mathbb{Z}_p\mathbb{Z}_p[u]$ additive codes can be generated by a matrix as follow:

$$\begin{pmatrix} S_2 & I_{k_1} & A_1 & A_2 \\ S_3 & 0 & uI_{k_2} & uA_3 \end{pmatrix},$$

where S_2, S_3, A_1, A_2, A_3 are Z_P -matrices. I_{k_1}, I_{k_2} is identity matrices.

According to generator matrices theorem, we know the matrices

$$\begin{pmatrix} I_{k_0} & S_{11} & S_{12} & S_{13} \\ S_2 & I_{k_1} & A_1 & A_2 \\ S_3 & 0 & uI_{k_2} & uA_3 \end{pmatrix},$$

is also generate the additive codes, where $S_1 = S_{11} + S_{12} + S_{13}$.

Next by applying necessary row and column operations to the above matrix, we obtain

$$\begin{pmatrix} I_{k_0} & 0 & S'_{12} & S'_{13} \\ 0 & I_{k_{11}} & A_1 & A_2 \\ 0 & 0 & uI_{k_{22}} & uA_3 \end{pmatrix},$$

Let $k'_0 = k_1 + k_{11}$, we can obtain the matrices

$$G = \begin{pmatrix} I_{k'_0} & A & B \\ 0 & uI_{k_1} & uD \end{pmatrix},$$

Finally, Let $k'_0 = k_0$, we reach to the claimed form. \square

The inner product for the vectors $v, w \in \mathbb{Z}_p\mathbb{Z}_p[u]$ is defined by

$$v \cdot w = u \left(\sum_{i=1}^{\alpha} v_i w_i \right) + \sum_{j=\alpha+1}^{\alpha+\beta} v_j w_j \in \mathbb{Z}_p + u\mathbb{Z}_p$$

Definition 3.3. Let C be a $\mathbb{Z}_p\mathbb{Z}_p[u]$ -additive code, The additive dual code of C , denote by C^\perp , and

$$C^\perp = \{w \in \mathbb{Z}_p^\alpha \times \mathbb{Z}_p[u]^\beta \mid v \cdot w = 0 \text{ for all } v \in C\}.$$

Theorem 3.4. Let C be a $\mathbb{Z}_p\mathbb{Z}_p[u]$ additive code of type $(p; \alpha, \beta; k_0, k_1)$ with the standard form matrix defined in Equation (1), Then the generator matrix for the additive dual code C^\perp is given by

$$H = \begin{pmatrix} -B^t + D^t A^t & -D^t & I_{n-k_0-k_1} \\ uA^t & -uI_{k_1} & 0 \end{pmatrix}, \quad (2)$$

Proof Denote the code with generator matrix (2) by C' . Since $HG' = 0$, clearly $C' \in C^\perp$. Let $c = (c_1, c_2, \dots, c_n) \in C^\perp$. After adding a linear combination of the first $n - k_0 - k_1$ row of (2) to c , we obtain a codeword is of the form

$$c' = (c_1, c_2, \dots, c_{k_0}, c_{k_0+1}, \dots, c_{k_0+k_1}, 0, \dots, 0) \in C^\perp$$

Since c' is orthogonal to the last k_1 rows of (1), so we can adding a certain linear combination of the last k_1 row of (2) to c' . Similar, we obtain a codeword is of the form

$$c'' = (c_1, c_2, \dots, c_{k_0}, 0, \dots, 0) \in C^\perp$$

Since c'' is orthogonal to the first k_0 rows of (1), so we can obtain $c_1 = c_2 = \dots = c_k = 0$. so $c \in C'$, $C^\perp \in C'$. Therefore H is the generator matrix of the additive dual code C^\perp . \square

Example 3.5. Let C be a $\mathbb{Z}_p\mathbb{Z}_p[u]$ -additive code of type $(3; 1, 4; 2, 2)$ with the standard form generator matrix:

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 2 & 0 \\ 0 & 0 & u & 0 & 2u \\ 0 & 0 & 0 & u & 0 \end{pmatrix} \quad (3)$$

Then, the parity-check matrix of C as given:

$$H = \begin{pmatrix} 2 & 0 & 1 & 0 & 1 \\ 0 & 0 & 2u & 0 & 0 \\ u & 2u & 0 & 2u & 0 \end{pmatrix} \quad (4)$$

And it's clear that C^\perp is of type $(3; 1, 4; 1, 2)$.

Notice that the number of codewords cannot given by the additive code of type.

4 The gray map

In this part of the paper, we study the MacWilliams identity for $\mathbb{Z}_p\mathbb{Z}_p[u]$ -additive code, the results is similar to $p = 2$ [3], and a Gray map Φ is given, we found the Gray map Φ is a distance preserving map from $(\mathbb{Z}_p\mathbb{Z}_p[u], \text{Gray distance})$ to $(\mathbb{Z}_p^{\alpha+2\beta}, \text{Hamming distance})$, and it is also a weight preserving map.

In the Preliminaries, we also define a Gray map ψ from R to Z_p^2 in the following way.

$$\begin{aligned} \psi : R &\rightarrow Z_p^2 \\ (a + ub) &\rightarrow (b, a + b). \end{aligned}$$

At the same time, in definition 3.1., we given a map Φ , it is from $\mathbb{Z}_p^\alpha \times \mathbb{Z}_p[u]^\beta$ to \mathbb{Z}_p^n defined as

$$\Phi(a, b) = (a_0, a_1, \dots, a_{\alpha-1}, \psi(b_0), \psi(b_1), \dots, \psi(b_{\beta-1}))$$

for all $a = (a_0, a_1, \dots, a_{\alpha-1}) \in \mathbb{Z}_p^\alpha$, $b = (b_0, b_1, \dots, b_{\beta-1}) \in \mathbb{Z}_p[u]^\beta$.

Let C be an additive code and assume $n = \alpha + 2\beta$, the weight enumerator of an additive code C is defined by

$$W(x, y) = \sum_{c \in C} x^{n-w(c)} y^{w(c)}.$$

Theorem 4.1. Let C be a $\mathbb{Z}_p\mathbb{Z}_p[u]$ -additive code, and C^\perp be its dual code, then their weight enumerators $W_G(x, y)$ and $W_{G^\perp}(x, y)$ are connected by the MacWilliams identity:

$$W_{G^\perp}(x, y) = \frac{1}{|C|} W_G(X + (q-1)Y, X - Y)$$

Proof Similar to the proof of [3, theorem 3.3]. \square

Let F_p^* is a multiplication group with nonzero elements, where p is an odd prime. Next we definition a Gray weight $W_G(c)$ for $c = (c_1, c_2, \dots, c_n)$ in the following way:

$$W_G(c) = \sum_{i=0}^{n-1} W_G(c_i)$$

where

$$W_G(c_i) = \begin{cases} 0, & \text{if } c_i = 0, \\ 2, & \text{if } c_i = a + u(p-b), a, b \in F_p^* \text{ and } a \neq b, \\ 1, & \text{others.} \end{cases}$$

This gray weight function defines also a gray distance function

$$d_G(x, y) = W_G(x - y)$$

The Hamming weight of a weight of n -tuples is the number of its nonzero entries. The Hamming distance between two n -tuples is defined as the Hamming weight of their difference. Denote the Hamming weight of a weight of a p -ary vector x by $W_H(x)$ and the Hamming distance between two p -ary vectors x and y of the same length by $d_H(x, y)$, and we have $W_H(x - y) = d_H(x, y)$.

Since $\forall c = (c_1, c_2, \dots, c_n) \in \mathbb{Z}_p\mathbb{Z}_p[u]$. We have

$$W_H(\Phi(c_i)) = \begin{cases} 0, & \text{if } c_i = 0, \\ 2, & \text{if } c_i = a + u(p-b), a, b \in F_p^* \text{ and } a \neq b, \\ 1, & \text{others.} \end{cases}$$

Clearly, $W_G(c_i) = W_H(\Phi(c_i)) \forall c_i \in \mathbb{Z}_p, i \in (1, 2, \dots, n)$. \square

Theorem 4.2. The Gray map Φ is a weight preserving map from

$$(\mathbb{Z}_p^\alpha \mathbb{Z}_p[u]^\beta, \text{Gray weight}) \text{ to } (\mathbb{Z}_p^{\alpha+2\beta}, \text{Hamming weight})$$

i.e.

$$W_G(c) = W_H(\Phi(c)) \text{ for } \forall c \in \mathbb{Z}_p\mathbb{Z}_p[u]. \quad (5)$$

and Φ is a distance preserving map from

$$(\mathbb{Z}_p^\alpha \mathbb{Z}_p[u]^\beta, \text{Gray distance}) \text{ to } (\mathbb{Z}_p^{\alpha+2\beta}, \text{Hamming distance})$$

i.e.

$$d_G(x, y) = d_H(\Phi(x), \Phi(y)) \quad \text{for } \forall x, y \in \mathbb{Z}_p \mathbb{Z}_p[u]. \quad (6)$$

Proof Let $\forall c = (c_1, c_2, \dots, c_\alpha, c_{\alpha+1}, \dots, c_{\alpha+\beta}) \in \mathbb{Z}_p^\alpha \mathbb{Z}_p[u]^\beta$, where $c_i \in \mathbb{Z}_p^\alpha, i = 1, 2, \dots, \alpha$. $c_{\alpha+i} = r_i + uq_i \in \mathbb{Z}_p[u]^\beta, i = 1, 2, \dots, \beta$. by the grap map Φ we obtain:

$$\begin{aligned} \Phi(c) &= (c_1, c_2, \dots, \psi(c_\alpha), \psi(c_{\alpha+1}), \dots, \psi(c_{\alpha+\beta})) \\ &= (c_1, c_2, \dots, c_\alpha, q_1, q_2, \dots, q_\beta, q_1 + r_1, q_2 + r_2, \dots, q_\beta + r_\beta) \end{aligned}$$

$$\begin{aligned} W_H(\Phi(c)) &= W_H(c_1, c_2, \dots, c_\alpha, q_1, q_2, \dots, q_\beta, q_1 + r_1, q_2 + r_2, \dots, q_\beta + r_\beta) \\ &= \sum_{i=1}^{\alpha} W_H(c_i) + \sum_{i=1}^{\beta} W_H(q_i, q_i + r_i) \\ &= \sum_{i=1}^{\alpha} W_H(c_i) + \sum_{i=1}^{\beta} W_H(\psi(c_{\alpha+i})) \\ &= \sum_{i=1}^{\alpha} W_G(c_i) + \sum_{i=1}^{\beta} W_G(c_{\alpha+i}) \\ &= \sum_{i=1}^{\alpha+\beta} W_G(c_i) = W_G(c) \end{aligned}$$

Therefore we have (5). Similarly, we also can deduce (6), the proof is omitted. \square

5 The structure of $\mathbb{Z}_p \mathbb{Z}_p[u]$ -additive cyclic code

In this part of the paper, we introduce the definition of a additive cyclic code and some algebraic structure. A code C is cyclic if and only if its polynomial representation is an ideal.

Let $R_{\alpha,\beta}[x] = \frac{\mathbb{Z}_p[x]}{\langle x^\alpha - 1 \rangle} \times \frac{\mathbb{Z}_p[x]}{\langle x^\beta - 1 \rangle}$.

Definition 5.1. A additive code C is called a $\mathbb{Z}_p \mathbb{Z}_p[u]$ -additive cyclic code if any cyclic shift of a codeword is also a code. i.e.,

$$(a_0, a_1, \dots, a_{\alpha-1}, b_0, b_1, \dots, b_{\beta-1}) \in C \Rightarrow (a_{\alpha-1}, a_0, \dots, a_{\alpha-2}, b_{\beta-1}, b_0, \dots, b_{\beta-2}) \in C.$$

Theorem 5.2. If C be any $\mathbb{Z}_p \mathbb{Z}_p[u]$ -additive cyclic code, then C^\perp is also cyclic.

Proof Let C be any $\mathbb{Z}_p^\alpha \mathbb{Z}_p[u]^\beta$ -additive cyclic code. Suppose $v = (a_0, a_1, \dots, a_{\alpha-1}, b_0, b_1, \dots, b_{\beta-1}) \in C^\perp$, for any codeword $w = (d_0, d_1, \dots, d_{\alpha-1}, e_0, e_1, \dots, e_{\beta-1}) \in C$ we have

$$v \cdot w = u \left(\sum_{i=0}^{\alpha-1} a_i d_i \right) + \sum_{j=0}^{\beta-1} b_j e_j = 0$$

Let S is a cyclic shift, and $j = \text{lcm}(\alpha, \beta)$. Then we have $S(v) = (a_{\alpha-1}, a_0, \dots, a_{\alpha-2}, b_{\beta-1}, b_0, \dots, b_{\beta-2})$ and $S^j(w) = w$ for any $w \in C$. Since C be any $\mathbb{Z}_p^\alpha \mathbb{Z}_p^\beta$ -additive cyclic code, So we have

$$S^{j-1}(w) = (d_1, d_2, \dots, d_{\alpha-1}, d_0, e_1, e_2, \dots, e_{\beta-1}, e_0) \in C$$

Hence

$$\begin{aligned} 0 &= v \cdot S^{j-1}(w) = u(a_0 d_1 + a_1 d_2 + \dots + a_{\alpha-2} d_{\alpha-1} + a_{\alpha-1} d_0) \\ &\quad + (b_0 e_1 + b_1 e_2 + \dots + b_{\beta-2} e_{\beta-1} + b_{\beta-1} e_0) \\ &= u(a_{\alpha-1} d_0 + a_0 d_1 + \dots + a_{\alpha-2} d_{\alpha-1}) \\ &\quad + (b_{\beta-1} e_0 + b_1 e_2 + \dots + b_{\beta-2} e_{\beta-2}) \\ &= S(v) \cdot w \end{aligned}$$

Therefore, we have $S(v) \in C^\perp$, so C^\perp is a cyclic code. \square

Let C be a $\mathbb{Z}_p \mathbb{Z}_p[u]$ -additive cyclic code, for any codeword $c = (a_0, a_1, \dots, a_{\alpha-1}, b_0, b_1, \dots, b_{\beta-1}) \in C$ can be representation with a polynomial, i.e.,

$$c(x) = (a_0 + a_1 x + \dots + a_{\alpha-1} x^{\alpha-1}, b_0 + b_1 x + \dots + b_{\beta-1} x^{\beta-1}) = (a(x), b(x)) \in R_{\alpha, \beta}[x].$$

Similarly. In preliminaries, we introduce a new scalar multiplication. Now, we have the following multiplication:

$$(1) \forall c_1(x) = (a_1(x), b_1(x)), c_2(x) = (a_2(x), b_2(x)) \in R_{\alpha, \beta}[x],$$

$$c_1(x)c_2(x) = (a_1(x)a_2(x), b_1(x)b_2(x))$$

$$(2) \forall c_1(x) = (a_1(x), b_1(x)) \in R_{\alpha, \beta}[x], c_2(x) = r(x) + uq(x) \in R[x], \text{ where } r(x), q(x) \in \mathbb{Z}_p[x],$$

$$c_1(x)c_2(x) = (a_1(x)r(x), b_1(x)c_2(x))$$

$$(3) \forall c_1(x) = (a_1(x), b_1(x)) \in R_{\alpha, \beta}[x], c_2(x) \in \mathbb{Z}_p[x],$$

$$c_1(x)c_2(x) = (a_1(x)c_2(x), b_1(x)c_2(x))$$

Clearly, definition 5.1 is equivalent to

$$\begin{aligned} c(x) &= (a_0 + a_1 x + \dots + a_{\alpha-1} x^{\alpha-1}, b_0 + b_1 x + \dots + b_{\beta-1} x^{\beta-1}) \in R_{\alpha, \beta}[x]. \\ \implies xc(x) &= (a_{\alpha-1} + a_0 x + \dots + a_{\alpha-2} x^{\alpha-1}, b_{\beta-1} + b_0 x + \dots + b_{\beta-2} x^{\beta-1}) \in R_{\alpha, \beta}[x]. \end{aligned}$$

Now, we define the homomorphism mapping:

$$\begin{aligned} \Psi : R_{\alpha, \beta}[x] &\longrightarrow R[x] \\ \Psi(c(x)) &= \Psi(a(x), b(x)) = b(x) \end{aligned}$$

It is clear that $\text{Image}(\Psi)$ is an ideal in the ring $\frac{R[x]}{\langle x^\beta - 1 \rangle}$ and $\ker(\Psi)$ is also an ideal over $\mathbb{Z}_p[x]$. And note that

$$\text{Image}(\Psi) = \{b(x) \in R[x] : (a(x), b(x)) \in R_{\alpha, \beta}[x]\}$$

$$\ker(\Psi) = \{(a(x), 0) \in R_{\alpha, \beta}[x] : a(x) \in \frac{\mathbb{Z}_p[x]}{x^\alpha - 1}\}$$

By using the characterization in [14], we have

$$\text{Image}(\Psi) = \langle g(x) + up(x), uq(x) \rangle$$

where $g(x), p(x), q(x) \in \frac{R[x]}{\langle x^\beta - 1 \rangle}$, $q(x) \mid g(x) \mid (x^\beta - 1)$ and $q(x) \mid p(x) \frac{x^\beta - 1}{g(x)}$.

Similarly,

$$\ker(\Psi) = \langle f(x), 0 \rangle$$

where $f(x) \in \frac{Z_p[x]}{x^\alpha - 1}$ and $f(x) \mid (x^\alpha - 1)$.

According to the homomorphism map theorem we have:

$$C/\ker(\Psi) \cong \langle g(x) + up(x), uq(x) \rangle.$$

Hence, we have

$$(h(x), (g(x) + up(x), uq(x))) \in C$$

where $\Psi(h(x), (g(x) + up(x), uq(x))) = (g(x) + up(x), uq(x))$.

By these discussion, it is easy to see that any $\mathbb{Z}_p\mathbb{Z}_p[u]$ -additive cyclic code can be generated by two elements of the form $(h(x), (g(x) + up(x), uq(x)))$ and $(f(x), 0)$.

Corollary 5.3. Let C be a $\mathbb{Z}_p\mathbb{Z}_p[u]$ -additive cyclic code. Then C is an ideal in $R_{\alpha,\beta}[x]$ which can be generated by

$$C = ((f(x), 0), (h(x), (g(x) + up(x), uq(x)))).$$

where $q(x) \mid g(x) \mid (x^\beta - 1)$, $q(x) \mid p(x) \frac{x^\beta - 1}{g(x)}$. \square

Corollary 5.4. Let $C = ((f(x), 0), (h(x), (g(x) + up(x), uq(x))))$ is a $\mathbb{Z}_p\mathbb{Z}_p[u]$ -additive cyclic code, then we may assume that $f(x) \mid h(x) \frac{x^\beta - 1}{l(x)}$ where $l(x) = \text{lcm}(p(x), q(x))$.

Proof (1) Since $\Psi(\frac{x^\beta - 1}{l(x)}(h(x), (g(x) + up(x), uq(x)))) = \Psi((\frac{x^\beta - 1}{l(x)} * h(x), 0)) = 0$.

Hence $(\frac{x^\beta - 1}{l(x)} * h(x), 0) \in \ker(\Psi) \subseteq C$ and $f(x) \mid h(x) \frac{x^\beta - 1}{l(x)}$. \square

As a consequence to this corollary, we classify the structure of the additive cyclic code into three categories by the following theorem.

Theorem 5.5. Let C be a $\mathbb{Z}_p\mathbb{Z}_p[u]$ -additive cyclic code. Then C can be identified as following:

(1) $C = ((f(x), 0)$, where $f(x) \in \frac{Z_p[x]}{x^\alpha - 1}$.

(2) $C = (h(x), (g(x) + up(x), uq(x)))$, where $q(x) \mid g(x) \mid (x^\beta - 1)$ and $(x^\beta - 1) \mid p(x) \frac{x^\beta - 1}{g(x)}$.

(3) $C = ((f(x), 0), (h(x), (g(x) + up(x), uq(x))))$, where $q(x) \mid g(x) \mid (x^\beta - 1)$, $q(x) \mid p(x) \frac{x^\beta - 1}{g(x)}$, $f(x) \mid h(x) \frac{x^\beta - 1}{l(x)}$ and $l(x) = \text{lcm}(p(x), q(x))$. \square

Corollary 5.6. Let C be any $\mathbb{Z}_p\mathbb{Z}_p[u]$ -additive cyclic code. Then $\Phi(C)$ is an cyclic code of length $\alpha + 2\beta$ over Z_p .

Proof Let S is a cyclic shift. Since C be any $\mathbb{Z}_p\mathbb{Z}_p[u]$ -additive cyclic code. For any codeword

$$c = (a_0, a_1, \dots, a_{\alpha-1}, b_0, b_1, \dots, b_{\beta-1}) \in C$$

where $b_i = r_i + uq_i, i \in \{0, 1, 2, \dots, \beta - 1\}, a_i, r_i, q_i \in Z_p$.

We have

$$S(c) = (a_{\alpha-1}, a_0, \dots, a_{\alpha-2}, b_{\beta-1}, b_0, \dots, b_{\beta-2}) \in C$$

Then

$$\begin{aligned} \Phi(S(c)) &= (a_{\alpha-1}, a_0, \dots, a_{\alpha-2}, q_{\beta-1}, q_0, \dots, \\ &\quad q_{\beta-2}, q_{\beta-1} + r_{\beta-1}, q_0 + r_0, \dots, q_{\beta-2} + r_{\beta-2}) \in \Phi(C) \end{aligned}$$

Then by the Gray map we have:

$$\Phi(c) = (a_0, a_1, \dots, a_{\alpha-1}, q_0, q_1, \dots, q_{\beta-1}, q_0 + r_0, q_1 + r_1, \dots, q_{\beta-1} + r_{\beta-1}) \in \Phi(C).$$

Hence

$$\begin{aligned} S(\Phi(c)) &= (a_{\alpha-1}, a_0, \dots, a_{\alpha-2}, q_{\beta-1}, q_0, \dots, q_{\beta-2}, \\ &\quad q_{\beta-1} + r_{\beta-1}, q_0 + r_0, \dots, q_{\beta-2} + r_{\beta-2}) = \Phi(S(c)) \in \Phi(C). \end{aligned}$$

This proves that $\Phi(C)$ is an cyclic code of length $\alpha + 2\beta$ over Z_p . \square

6 Conclusion

In this paper, we studied $Z_p Z_p[u]$ -additive codes some property, including generator and parity check matrices for the codes. We fund the Gray map Φ is a distance preserving map and weight preserving map as well. At the end of the paper, we introduce the structure of $Z_p Z_p[u]$ -additive cyclic code. The studies makes this family of codes become widespread. we hope this family of codes haven more studies, such as constacyclic codes, depth distribution and other place. Due to this family of codes is newly introduced, some similar problems are still open here.

References

- [1] P.Delsarte, An algebraic approach to the association schemes of coding theory[R]. philips Research Rep Suppl,1973.
- [2] G.H. Norton, A.S., On the Hamming Distance of Linear Codes Over a Finite Chain Ring. IEEE Trans. Inform. Theory, VOL.46, NO.3, MAY 2000.
- [3] I.Aydogdu, T.Abualrub , I.Siap, On $Z_2 Z_2[u]$ additive codes, Int.J.Comput.Math.2014.doi: 10.1080/00207160.2013.859854
- [4] I.Aydogdu , I.Siap , On $Z_{p^r} Z_{p^s}$ -additive codes, Linear and Multilinear Algebra, 2015. Vol.63. No.10.2089-2102.
- [5] RC.Singleton, Maximum distance q -ary codes. IEEE Trans. Inform. Theory. 1964; 10:116-118.
- [6] J.Borges, C.Fernández, J.Pujol, M.Villanueva, $Z_2 Z_4$ -linear codes and duality. VJMDA, pp.171-177, Ciencias, 23. Secr. Publ. intercamb. Ed., Valladolid (2006).
- [7] M.Bilal, J.Borges, S.T.Dougherty, C.Fernández, Maximum distance separable codes over Z_4 and $Z_2 \times Z_4$. Des. codes cryptogr. (2011) 61:31-40.

- [8] B.Jürgen, Cyclic additive codes. Journal of Algebra 372(2012)661-672.
- [9] I.Aydogdu and I.Siap, The structure of $Z_2Z_{2^s}$ -additive code: Bounds on the minimum distance, Appl.Math.Inform.Sci.7(6)(2013),pp.2271-2278.
- [10] H.Rifa, J.Rifa, and L.Ronquillo, Perfect Z_2Z_4 -linear codes in steganography, Comput.Res.Reposit.,Vol.abs/1002.0(2010).
- [11] J.Rifa, L.Ronquillo, Product Perfect Z_2Z_4 -linear codes in steganography.ISITA,Taichung, Taiwan,October 2010,pp.696-701.
- [12] F.J.MacWilliams, N.J.A. Solane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1997.
- [13] Z.X.Wan, Quaternary Codes, World Scientific, Singapore, 1997.
- [14] X.S.Liu, H.L.Liu, Cyclic Code over $F_2 + uF_2 + vF_2$, Chin.Quart.J.of Math.2014,29(2):189-194.
- [15] T.Abualrub, I.Siap, N.Aydin, Z_2Z_4 -Additive Cyclic Codes ,IEEE Trans.Inform.Theory. VOL.60.NO.3.MARCH 2014.